

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Snap Inc.  
2772 Donald Douglas Loop North  
Santa Monica, CA 90405

Case No. 2:20-mj-344

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment Alocated in the Central District of California, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1951	Interference with Interstate Commerce by Robbery
18 USC 924(c)(1)(A)(ii)	Brandish a Firearm while Committing a Crime of Violence

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Brian V. Boesch* TFO 6651  
Applicant's signature

Task Force Officer Brian V. Boesch  
Printed name and title

Sworn to before me and signed in my presence.

Date:

5-12-20

City and state: Columbus, OH

*W. Vascura*  
Judge's signature

Magistrate Judge Chelsey M. Vascura  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
abdi\_ali35; pina\_33; momotheboss2015;  
thatnigga\_hanad THAT ARE STORED AT  
PREMISES CONTROLLED BY Snapchat,  
located in Santa Monica, CA

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Task Force Officer (TFO) Brian V. Boesch , being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Snap Inc., an [electronic communications service/remote computing service provider] headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Task Force Officer (TFO) with the Bureau of Alcohol, Tobacco, Firearms and Explosives, and have been since July 6, 2014. Prior to joining the task force, I was assigned as a robbery detective with the Columbus Division of Police for 8 ½ years. During the past 14

years, I have investigated thousands of robberies and prosecuted them both in state and federal court. During these investigations, I have come to understand that criminals utilize their cell phones to communicate with other suspects; use internet searches to identify robbery targets; use mapping applications to locate their targets; discuss the proceeds from robberies; take photos of the evidence and share it using social media applications on their phones; and these devices will log the suspect locations at and around the time of the crimes they are committing. A forensic download of the device provides all of the above information, including other items stored on the phone that may be of evidentiary value to the investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1951 18 U.S.C. § 924(c)(1)(A)(ii) and have been committed by Abdifatah A. MOHAMED. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).] and “is in . . . a district in

which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii)

### **PROBABLE CAUSE**

6. On December 16, 2019 at approximately 2:40pm Detective Brad Slone #1712 was notified by Officer James Schiering #1717 of an aggravated robbery at the CRMD ice cream parlor, located at 1190 N. High St. Officer Schiering stated the suspect entered the business and asked the victim for change to put in the parking meter. Officer Schiering stated the victim opened the register and the suspect pulled out a gun pointing it at her and demanding all the money from the register. Officer Schiering stated the victim complied and the suspect left on foot southbound on N. High St. Officer Schiering stated the incident was captured on surveillance video. Officer James Schiering #1717 documented the incident under report #191046795.

Ms. Doung described the suspect as a male black, early to mid 20's, 5'6", normal build, light skin, wearing a green jacket, yellow Kappa hoody, black jeans, white/lt. blue shoes and a American flag bandanna over his face. Ms. Doung described the gun as a black semi-automatic, possibly a 9mm.

Det. Jason Wood canvassed nearby businesses and discovered the suspect entered The Garden located at 1174 N. High St. just before he committed the robbery. The suspect was wearing the same clothing as when he robbed the CRMD store moments later. Det. Wood watched surveillance video and observed the suspect place his right hand on the glass door to exit the business. CSSU Detectives responded and collected latent prints from the area touched by the suspect.

On January 5, 2020 Det. Slone received the crime lab report showing latent print 1A recovered from the door of The Garden was a match to the right thumb of Abdifatah A. MOHAMED (m/b, 3/21/2000, FBI# R89WF09TT). Comparing the surveillance video and the photos from CSSU the thumb print was lifted from the same area the suspect placed his right thumb to open the door.

On January 20, 2020, TFO Boesch presented a complaint and affidavit to Southern District of Ohio Magistrate Judge Chelsey M. Vascura for an arrest warrant for MOHAMED. Judge Vascura signed the warrant, which was later entered into the National Crime Information Computer (NCIC).

On February 7, 2020, Siham Mohamed call the Columbus Division of Police to report that her ex-boyfriend, Abdifatah MOHAMED, had just shot at her and two other people over a dispute involving a cell phone. Detective Tim Pribe eventually filed state charges of Felonious Assault against MOHAMED.

On March 30, 2020, MOHAMED was arrested for his warrant. The Dublin Police Department arrested MOHAMED and seized a cell phone in his possession. They obtained a State of Ohio search warrant for his phone and conducted a forensic examination of the phone. They were able to obtain an extensive contact list of accounts that MOHAMED was friends with on Snapchat.

TFO Boesch began monitoring the phone calls MOHAMED made from the jail. MOHAMED primarily spoke to three (3) people; his mother, Anas Mohamed, and Hanad Dahir. During the recorded calls, MOHAMED tells Dahir to sign into his Snapchat account and make sure nothing is there. Dahir agrees. During another phone call with Dahir, MOHAMED directs Dahir to find his ex-girlfriend, Siham, which he does. MOHAMED and Siham talk directly to each other on Dahir's phone and appear to have reconciled. MOHAMED directs Siham to get into his Snapchat account and make sure nothing is there. He also directs her to contact Mohamed Sharif-Ali Mohamed via his Snapchat to take care of her because he knows about the situation.

During a conversation with Anan Mohamed, MOHAMED wonders why the ATF is involved and starts speaking in Somalian. During the time he was speaking in Somalian, TFO Boesch distinctly heard MOHAMED say, "Ice Cream".

During the discussions with all three individuals, the Snapchat application is mentioned extensively as a means for MOHAMED to communicate with several individuals that are, or may have knowledge of his criminal activity.

On April 23, 2020, TFO Boesch submitted preservation requests to Snapchat to preserve any content they may have on their servers for the four accounts:

MOHAMED – abd\_ali35

Siham Mohamed – pina\_033

Hanad Dahir – thatnigga\_hanad

Mohamed Mohamed – momotheboss2015

7. 4. Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos. Referred to as 'snaps', the company processes approximately 700 million of them every day on Apple's iOS and Google's Android operating systems. Snapchat users access the application frequently. According to marketing material provided by the company the average Snapchat user checks their account 14 times a day.

8. Snap Inc. is headquartered in Santa Monica, CA and owns and operates a free access social networking website of the same name that can be accessed at <http://www.snapchat.com>. Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos. Referred to as "snaps", the company processes approximately 700 million "snaps" each day.

9. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaved the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be send from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and "snaps" constitute "electronic communications" within the meaning of 18 U.S.C. § 3123. See 18 U.S.C. §§ 3127(1) and 2510(12).

10. "Our Stories" is a collection of user submitted "Snaps" from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a rave could all contribute to the same "Our Stories" collection by sharing their snaps, even if they do not know each other. Users can also view "Our Stories" events if they are not actually present at the event by subscribing to the story. In addition to "Our Stories", a Snapchat user can keep a



sort of photo/video diary using the “Story” feature. Each snap in a “Story” documents the user’s experience. Based on the user’s privacy settings, the photos and videos added to a “Story” can be viewed either by everyone on Snapchat or just the user’s friend. Stories are visible to other users for up to 24 hours.

11. In addition to photos, videos, “Snaps” and stories, “Snapcash” is an online money transfer service offered by Snapchat. The actual business platform is run by “SquareUp”, the distributor of a mobile credit card reader and application Square Register. Snapcash can be used to transfer money between Snapchat users using a linked, U.S. issued Visa or MasterCard debit card only; using credit cards is not permitted. Snapcash can only be sent to other users who have a linked debit card. Snapcash has a \$250 weekly limit but can be upgraded to a \$2,500 weekly limit. Users who upgrade have to provide their full name, date of birth, and Social Security number.

12. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

13. In general, providers like Snap, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an ACCOUNT. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers,

e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number).

14. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the ACCOUNT.

15. In some cases, ACCOUNT users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap, Inc. to disclose to the government copies of the records and other information



(including the content of communications) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

17. Based on the forgoing, I request that the Court issue the proposed search warrant.

18. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

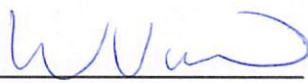
19. The government will execute this warrant by serving the warrant on Snap, Inc. Because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

 TFO  
6551

Brian V. Boesch  
Task Force Officer (TFO)  
Bureau of Alcohol, Tobacco, Firearms and  
Explosives

Subscribed and sworn to before me on May 12, 2020

  
Chelsey M. Vascara  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

**This warrant applies to information associated with:**

**Abd\_ali35**

**Pina\_033**

**Thatnigga\_hanad**

**Momotheboss2015**

**that are stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.**

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Snap Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Snap Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snap Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. (a) All stored communications and other files in your possession (to include, if available, account access information, event histories including dates and times, connection dates, times and locations, connection IP information, message content, graphics files, attachments, etc., further detailed below), whether physical, stored on electronic media, or temporarily extant on any computer or server, reflecting communications to or from Snapchat Accounts: “abd\_ali35”; “pina\_033”; “thatnigga\_hanad”; and “momotheboss2015”.

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) from the dates of **March 1, 2020 to April 23, 2020**;

c. The types of service utilized by the user;

d. All records or other information stored by an individual using the account, including:

- 1) Transmitter/Sender identifier (i.e. addresses and/or IP address);
- 2) Connection date and time;
- 3) Method of connection (telnet, ftp, http);
- 4) Data transfer volume;
- 5) User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
- 6) Account subscriber identification records;
- 7) Other user accounts associated with, referenced in or accessed by Snapchat Accounts: “abd\_ali35”; “pina\_033”; “thatnigga\_hanad”; and “momotheboss2015”
- 8) Address books, contact lists and “my friends” if available;
- 9) Records of files or system attributes accessed, modified, or added by the user.

e. All records pertaining to communications between Snap Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1951 and 18 U.S.C. 924(c)(1)(A)(ii) involving

**Abdifatah MOHAMED from 3/1/2020 to April 23, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:**

- (a) Chat messages that relate to armed business robberies, specifically the CRMD ice cream parlor; shooting at Siham Mohamed; or any other violent crime; photographs or videos shared that contain evidence of the above offenses;**
- (b) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).**
- (c) The identity of the person(s) who communicated with the user ID about matters relating to describe relevant offense conduct, including records that help reveal their whereabouts.**
- (d) Logs containing metadata about a user's Snaps, Stories, and Chats, but not the user's content.**
- (e) Location data may that be available for a Snapchat user who has turned on location services on their device and opted into location services in the app settings.**